Boolean Chaotic Encryption (BCE)

Wilbert Osmond
Gold Medalist in Computer Science (ICYS 2016 Romania)
Supervisor: Sungguh Ponten Aritonang, S.Kom., S.Pd
Chandra Kusuma High School, Indonesia - wilbertosmond@hotmail.co.id

One of the greatest breakthroughs in mathematical computation in this century has been the realization that even the simplest of dynamical systems may behave extremely unpredictable. Chaos theory exhibits a great sensitivity to initial conditions that a mere slight of difference on the input, will result to a widely diverging output. Chaotic computation literally scrambles bits that it appears to be nonsense and static, regarding to its high frequency and increasing speed in bifurcation within its chaotic regime. This is what encryption finds chaotic computation most useful to conceal messages, by thoroughly destroying the relationship between its input and output. Despite its seemingly randomness, it has a deterministic nature, regarding its fractal self-similarity from iterations, also helps the necessity of decryption. Another important factor that has to be considered is its speed, which is inversely proportional to its strength. This is why I have decided to apply the mathematical and exploited chaotic equation, which its simplicity is to assure the speed effectiveness and its dynamical unpredictability for the strength effectiveness, to encryption. However, converting mathematical chaos theory into an electronic circuit has also found itself troubles.

Boolean networks consist of randomly connected nodes, each of which has a binary state: on or off (1 or 0), which simplify the treatment of highly nonlinear systems. The state space of deterministic boolean networks with synchronous update is, however, finite, and thus, they cannot exhibit chaotic behaviour, as defined by an exponential sensitivity to initial conditions. One way of recovering non-periodic behavior is to update the state of the Boolean elements in an, at least seemingly, random order, in which chaos theory can be utilised. The chaotic binary state, I hypothesise, can be projected into logic gates electronic circuit for encryption.

For its efficient security assurance, further security analyses are to be carried out. First, avalanche effect analysis, to verify its exhibition of chaos' most prominent feature that is its sensitivity to initial conditions by how the input value should produce a completely different and widely diverging output even a single bit is altered. Subsequently, for its determination of chaotic region, its bifurcation diagram is to be shown as the visual analysis; whereas for the mathematical analysis, the Lyapunov exponent is to be tooled. Last but not least, time complexity to guarantee how fast mode of communication it can be. On the other hand, the practical prove as to if the encryption works, will be carried out in a simulator program.

Keywords*: chaos theory, encryption, boolean algebra, security analyses*